Semester 1 Examinations 2021/2022

Exam Code(s)	4BCT1, 4BP1
Exam(s)	B.Sc. Degree (Computer Science & Information Technology), Bachelor of Engineering (Electronic and Computer Engineering)
Module Code(s)	CT417
Module(s)	Software Engineering III
Paper No.	1
External Examiner(s)	Dr. Ramona Trestian
Internal Examiner(s)	Prof. Michael Madden *Dr. Matthias Nickles *Dr. Michael Schukat

Instructions: **Answer three questions in total.**

Answer **two** questions from Section A

AND

Answer **one** question from Section B

Duration	**2 hours**
No. of Pages	**5**
Discipline(s)	Computer Science
Course Co-ordinator(s)	Dr. Colm O'Riordan
Requirements	None

Section A (Formal Specification)

Answer any two questions from this section

Question 1

a) What is a *surjective function* (in the context of Z)? Support your explanation with an example of your own choice (in Z notation).

[5 marks]

b) You are given the following global variable and state schema for a part of a high-speed train booking system:

$trainCapacity : \mathbb{N}$

TrainBooking

$$booked : \mathbb{P}\ \text{PERSON}$$

$$\#booked \leq trainCapacity$$

b1) What would be a suitable initial state schema (initial state operation) in Z notation for this scenario?

[5 marks]

b2) Write Z specifications for the following two operations:

- Someone books a ticket
- Someone cancels a booking

Remark: it is *not* necessary to provide any error handling in your answer.

[10 marks]

PTO

Question 2

You are given the following state schema for a supermarket item (stock) management system. The supermarket *carries* a set of different items. Of the carried items, there are certain numbers currently available per each item (the *level* of that item). For example, the supermarket might carry kidney bean tins and croissants. The current number (level) of kidney bean tins available might be 30, the level of croissants might be 20.

SupermarketItems

$carried : \mathbb{P}\,\text{ITEM}$
$level : \text{ITEM} \pfun \mathbb{N}$

$\text{dom}\ level = carried$

a) Explain in your own words the precise meaning of the above specification.
[5 marks]

b) Provide a suitable initial state schema (initial state operation) in Z notation.
[5 marks]

c) Provide a Z specification for the operation of buying a given quantity of a given item.
Remark: it is *not* necessary to provide any error handling in your answer.
[10 marks]

PTO

Question 3

Consider the following description of (simplified) Association football (soccer) rules:

There are two teams with initially 11 field players per team. Additionally, each team has seven substitute players. The maximum number of substitutions per team is three. Each player can be shown the yellow card up to two times and the red card maximally once by the referee. When having been shown the yellow card twice or the red card once, the player is dismissed from the field with no substitution.

a) Create a suitable initial state schema (in Z notation) for the description above.
[7 marks]

b) Write Z specifications for the following operations:

- Show a player a red card.
- Show a player a yellow card.
- Query the current number of field players of a given team.

[13 marks]

PTO

Section B (Secure by Design)

Answer one questions from this section

Case Study for Question 4 and Question 5

Consider you have been instructed to develop a website for your local athletics club. The website has a "members only" section where users have to register / login, an online shop to buy merchandise, and a public online forum where registered users can post comments.

Question 4 (20 Marks)

Using the above case study discuss in some detail the following:

a) What type of cookies, their content / structure and attributes would you choose to support the above functionality? In your answer please explain the lifecycle of your chosen cookies. Provide code snippets where appropriate. (7 Marks)
b) Using concrete examples show how your website could be attacked via (i) reflected and (ii) persistent XSS attacks, and what the outcome of such an attack could be. (10 Marks)
c) Briefly discuss how your website could be hardened against XSS attacks. (3 Marks)

Question 5 (20 Marks)

Using the above case study discuss in some detail:

a) the inner workings of an SQL injection attack, and how such an attack could be used to retrieve or manipulate user credentials. (10 Marks)
b) how such attacks could be prevented. (3 Marks)
c) the benefits of password hashing to minimise the effect of injection attacks, thereby highlighting the characteristics of a good hash function. (3 Marks)
d) how dictionary attacks can be used to recover hashed passwords. (4 Marks)